

1 **CLAIMS**

2 What is claimed is:

3  
4 1. An optical data storage medium comprising:  
5 optically-readable material suitable for storing data therein; and  
6 stored within said optically-readable material, instructional data for an  
7 optical media content protection scheme, said instructional data being configured  
8 to cause logic associated with an optical media receiving device to operatively  
9 perform in accordance with said optical media content protection scheme when  
10 programmed using said instructional data and accessing associated content data  
11 stored on said optical data storage medium.

12  
13 2. The optical data storage medium as recited in Claim 1, wherein said  
14 optical media content protection scheme includes a digital rights management  
15 (DRM) protection scheme.

16  
17 3. The optical data storage medium as recited in Claim 2, wherein said  
18 DRM protection scheme includes at least one marking scheme selected from a  
19 group of marking schemes comprising a data-implemented water marking scheme  
20 and a data-implemented forensic marking scheme.

21  
22 4. The optical data storage medium as recited in Claim 1, further  
23 comprising at least one type of additional data stored within said optically-  
24 readable material, said type of additional data being selected from a group of  
25 additional data comprising substantially unique identifier data associated with said

1 optical data storage medium, licensing data associated with said optical data  
2 storage medium, and said content data.

3  
4 5. The optical data storage medium as recited in Claim 1, further  
5 comprising:

6 at least one optically-detectable authentication feature.

7  
8 6. The optical data storage medium as recited in Claim 5, wherein said  
9 optically-detectable authentication feature includes a plurality of optically-  
10 detectable authentication features forming a substantially unique pattern using at  
11 least one optically detectable material.

12  
13 7. The optical data storage medium as recited in Claim 6, wherein said  
14 optically detectable material includes at least one material selected from a group of  
15 optically detectable materials comprising an opaque material, a partially opaque  
16 material, a polymer-based material, and an epoxy-based material.

17  
18 8. The optical data storage medium as recited in Claim 6, wherein said  
19 plurality of optically-detectable authentication features form an optically-  
20 detectable certificate of authentication (COA).

21  
22 9. The optical data storage medium as recited in Claim 8, further  
23 comprising:

24 COA information data stored within said optically-readable material.  
25

1           10.    The optical data storage medium as recited in Claim 9, wherein said  
2 COA information data includes at least one type of data associated with said COA  
3 selected from a group of COA information data comprising raw optically-detected  
4 COA data, COA related plaintext data, and COA related signature data.

5  
6           11.    The optical data storage medium as recited in Claim 5, further  
7 comprising:

8           at least one top surface material and wherein at least one of the following  
9 occurs:

10                   said at least one optically-detectable authentication feature is formed  
11 on said top surface material;

12                   said at least one optically-detectable authentication feature is formed  
13 below said top surface material; and

14                   said at least one optically-detectable authentication feature extends  
15 at least partially into said top surface material.

16  
17           12.    An optical data storage medium comprising:  
18 optically-readable material suitable for storing data therein; and  
19 at least one optically-detectable non-data-based, physical authentication  
20 feature having a substantially unique pattern and comprising at least one optically  
21 detectable material.

22  
23           13.    The optical data storage medium as recited in Claim 12, wherein  
24 said optically detectable material includes at least one material selected from a  
25

1 group of optically detectable materials comprising an opaque material, a partially  
2 opaque material, a polymer-based material, and an epoxy-based material.

3  
4 14. The optical data storage medium as recited in Claim 12, wherein  
5 said authentication feature forms an optically-detectable certificate of  
6 authentication (COA).

7  
8 15. The optical data storage medium as recited in Claim 14, further  
9 comprising:

10 COA information data stored within said optically-readable material.

11  
12 16. The optical data storage medium as recited in Claim 15, wherein  
13 said COA information data includes at least one type of data associated with said  
14 COA selected from a group of COA information data comprising raw optically-  
15 detected COA data, COA related plaintext data, and COA related signature data.

16  
17 17. The optical data storage medium as recited in Claim 12, further  
18 comprising at least one top surface material, and wherein at least one of the  
19 following statements is true:

20 said authentication feature is formed on said top surface material;

21 said authentication feature is formed below said top surface material;

22 and

23 said authentication feature is formed so as to extend at least partially  
24 into said top surface material.

1           18.    An apparatus comprising:  
2           means for storing instructional data for an optical media content protection  
3 scheme within an optical data storage medium, said instructional data being  
4 configured to cause logic associated with an optical media receiving device to  
5 operate in accordance with said optical media content protection scheme when  
6 programmed using said instructional data and accessing associated content data  
7 stored on said optical data storage medium.

8  
9           19.    The apparatus as recited in Claim 18, wherein said optical media  
10 content protection scheme includes a digital rights management (DRM) protection  
11 scheme.

12  
13           20.    The apparatus as recited in Claim 19, wherein said DRM protection  
14 scheme includes at least one marking scheme selected from a group of marking  
15 schemes comprising a data-implemented water marking scheme and a data-  
16 implemented forensic marking scheme.

17  
18           21.    The apparatus as recited in Claim 18, further comprising:  
19           means for storing at least one type of additional data within said optical  
20 data storage medium, said type of additional data being selected from a group of  
21 additional data comprising substantially unique identifier data associated with said  
22 optical data storage medium, licensing data associated with said optical data  
23 storage medium, and said content data.

1        22.    The apparatus as recited in Claim 18, further comprising:  
2        means for causing at least one optically-detectable authentication feature to  
3        be included in said optical data storage medium.

4  
5        23.    The apparatus as recited in Claim 22, wherein said optically-  
6        detectable authentication feature includes a plurality of optically-detectable  
7        authentication features forming a substantially unique pattern using at least one  
8        optically detectable material.

9  
10       24.    The apparatus as recited in Claim 23, wherein said optically  
11       detectable material includes at least one material selected from a group of optically  
12       detectable materials comprising an opaque material, a partially opaque material, a  
13       polymer-based material, and an epoxy-based material.

14  
15       25.    The apparatus as recited in Claim 23, wherein said plurality of  
16       optically-detectable authentication features form an optically-detectable certificate  
17       of authentication (COA).

18  
19       26.    The apparatus as recited in Claim 25, further comprising:  
20       means for storing COA information data within said optical data storage  
21       medium.

22  
23       27.    The apparatus as recited in Claim 26, wherein said COA information  
24       data includes at least one type of data associated with said COA selected from a  
25

1 group of COA information data comprising raw optically-detected COA data,  
2 COA related plaintext data, and COA related signature data.

3  
4 28. The apparatus as recited in Claim 27, further comprising:  
5 means for generating said COA information data.

6  
7 29. The apparatus as recited in Claim 22, further comprising:  
8 wherein said optical data storage medium includes at least one top surface  
9 material, and further comprising at least one means for causing at least one of the  
10 following functions to occur:

11 forming said at least one optically-detectable authentication feature  
12 on said top surface material;

13 forming at least one optically-detectable authentication feature  
14 below said top surface material; and

15 forming said at least one optically-detectable authentication feature  
16 such that said optically-detectable authentication feature extends at least  
17 partially into said top surface material.

18  
19 30. An apparatus comprising:

20 means for forming at least one optically-detectable non-data-based,  
21 physical authentication feature as part of an optical data storage medium, said  
22 authentication feature having a substantially unique pattern and comprising at least  
23 one optically detectable material.

1        31. The apparatus as recited in Claim 30, wherein said optically  
2 detectable material includes at least one material selected from a group of optically  
3 detectable materials comprising an opaque material, a partially opaque material, a  
4 polymer-based material, and an epoxy-based material.

5  
6        32. The apparatus as recited in Claim 30, wherein said authentication  
7 feature is an optically-detectable certificate of authentication (COA).

8  
9        33. The apparatus as recited in Claim 32, further comprising:  
10 means for storing COA information data within said optical data storage  
11 medium.

12  
13        34. The apparatus as recited in Claim 33, wherein said COA information  
14 data includes at least one type of data associated with said COA selected from a  
15 group of COA information data comprising raw optically-detected COA data,  
16 COA related plaintext data, and COA related signature data.

17  
18        35. The apparatus as recited in Claim 30, wherein said optical data  
19 storage medium includes at least one top surface material, and further comprising  
20 at least one means for causing at least one of the following functions to occur:

21            forming said at least one optically-detectable authentication feature  
22            on said top surface material;

23            forming at least one optically-detectable authentication feature  
24            below said top surface material; and  
25



1           forming said at least one optically-detectable authentication feature  
2           such that said optically-detectable authentication feature extends at least  
3           partially into said top surface material.

4  
5           36.    An apparatus comprising:  
6           a data storage device configurable to write data to an optical data storage  
7           medium; and  
8           logic operatively coupled to said configured to said data storage device and  
9           configured to cause said data storage device to record instructional data for an  
10          optical media content protection scheme within said optical data storage medium,  
11          said instructional data being configured to cause logic associated with an optical  
12          media receiving device to operate in accordance with said optical media content  
13          protection scheme when programmed using said instructional data and accessing  
14          associated content on said an optical data storage medium.

15  
16          37.    The apparatus as recited in Claim 36, wherein said optical media  
17          content protection scheme includes digital rights management (DRM) protection  
18          scheme.

19  
20          38.    The apparatus as recited in Claim 37, wherein said DRM protection  
21          scheme includes at least one marking scheme selected from a group of marking  
22          schemes comprising a data-implemented water marking scheme and a data-  
23          implemented forensic marking scheme.

1           39.    The apparatus as recited in Claim 36, wherein said logic is further  
2 configured to cause said data storage device to record at least one type of  
3 additional data within said optical data storage medium, said type of additional  
4 data being selected from a group of additional data comprising substantially  
5 unique identifier data associated with said optical data storage medium, licensing  
6 data associated with said optical data storage medium, and content data.

7  
8           40.    The apparatus as recited in Claim 36, wherein said optical data  
9 storage medium further includes at least one optically-detectable authentication  
10 feature.

11  
12           41.    The apparatus as recited in Claim 40, wherein said data storage  
13 device is further configurable to detect said at least one optically-detectable  
14 authentication feature and provide resulting authentication feature information to  
15 said logic.

16  
17           42.    The apparatus as recited in Claim 40, wherein said optically-  
18 detectable authentication feature includes a plurality of optically-detectable  
19 authentication features forming a substantially unique pattern using at least one  
20 optically detectable material.

21  
22           43.    The apparatus as recited in Claim 41, wherein said plurality of  
23 optically-detectable authentication features form an optically-detectable certificate  
24 of authentication (COA).  
25

1           44.    The apparatus as recited in Claim 43, wherein said logic is further  
2 configured to cause said data storage device to record COA information data  
3 within said optical data storage medium.

4  
5           45.    The apparatus as recited in Claim 44, wherein said COA information  
6 data includes at least one type of data associated with said COA selected from a  
7 group of COA information data comprising raw optically-detected COA data,  
8 COA related plaintext data, and COA related signature data.

9  
10          46.    An apparatus comprising:  
11           an authentication feature forming mechanism configured to apply  
12 authentication feature forming material to an optical data storage medium so as to  
13 form at least one optically-detectable non-data-based, physical authentication  
14 feature as part of said optical data storage medium, said authentication feature  
15 having a substantially unique pattern and comprising at least one optically  
16 detectable material.

17  
18          47.    The apparatus as recited in Claim 46, wherein said optically  
19 detectable material includes at least one material selected from a group of optically  
20 detectable materials comprising an opaque material, a partially opaque material, a  
21 polymer-based material, and an epoxy-based material.

22  
23          48.    The apparatus as recited in Claim 46, wherein said authentication  
24 feature is an optically-detectable certificate of authentication (COA).  
25

1           49.    A method comprising:  
2           storing instructional data for an optical media content protection scheme  
3           within an optical data storage medium, said instructional data being configured to  
4           cause logic associated with an optical media receiving device to operate in  
5           accordance with said optical media content protection scheme when programmed  
6           using said instructional data and accessing associated content data stored on said  
7           optical data storage medium.

8  
9           50.    The method as recited in Claim 49, wherein said optical media  
10          content protection scheme includes a digital rights management (DRM) protection  
11          scheme.

12  
13          51.    The method as recited in Claim 50, wherein said DRM protection  
14          scheme includes at least one marking scheme selected from a group of marking  
15          schemes comprising a data-implemented water marking scheme and a data-  
16          implemented forensic marking scheme.

17  
18          52.    The method as recited in Claim 49, further comprising:  
19          storing at least one type of additional data within said optical data storage  
20          medium, said type of additional data being selected from a group of additional  
21          data comprising substantially unique identifier data associated with said optical  
22          data storage medium, licensing data associated with said optical data storage  
23          medium, and said content data.

24  
25          53.    The method as recited in Claim 49, further comprising:

1 causing at least one optically-detectable authentication feature to be  
2 included in said optical data storage medium.

3  
4 54. The method as recited in Claim 53, wherein said optically-detectable  
5 authentication feature includes a plurality of optically-detectable authentication  
6 features forming a substantially unique pattern using at least one optically  
7 detectable material.

8  
9 55. The method as recited in Claim 54, wherein said optically detectable  
10 material includes at least one material selected from a group of optically detectable  
11 materials comprising an opaque material, a partially opaque material, a polymer-  
12 based material, and an epoxy-based material.

13  
14 56. The method as recited in Claim 54, wherein said plurality of  
15 optically-detectable authentication features form an optically-detectable certificate  
16 of authentication (COA).

17  
18 57. The method as recited in Claim 56, further comprising:  
19 storing COA information data within said optical data storage medium.

20  
21 58. The method as recited in Claim 57, wherein said COA information  
22 data includes at least one type of data associated with said COA selected from a  
23 group of COA information data comprising raw optically-detected COA data,  
24 COA related plaintext data, and COA related signature data.

1        59.    The method as recited in Claim 58, further comprising:  
2        generating said COA information data.

3  
4        60.    The method as recited in Claim 53, further comprising:  
5        wherein said optical data storage medium includes at least one top surface  
6        material, causing at least one of the following acts to occur:

7                forming said at least one optically-detectable authentication feature  
8                on said top surface material;

9                forming at least one optically-detectable authentication feature  
10              below said top surface material; and

11              forming said at least one optically-detectable authentication feature  
12              such that said optically-detectable authentication feature extends at least  
13              partially into said top surface material.

14  
15        61.    A method comprising:

16              forming at least one optically-detectable non-data-based, physical  
17              authentication feature as part of an optical data storage medium, said  
18              authentication feature having a substantially unique pattern and comprising at least  
19              one optically detectable material.

20  
21        62.    The method as recited in Claim 61, wherein said optically detectable  
22        material includes at least one material selected from a group of optically detectable  
23        materials comprising an opaque material, a partially opaque material, a polymer-  
24        based material, and an epoxy-based material.

1           63.    The method as recited in Claim 61, wherein said authentication  
2 feature is an optically-detectable certificate of authentication (COA).

3  
4           64.    The method as recited in Claim 63, further comprising:  
5 storing COA information data within said optical data storage medium.

6  
7           65.    The method as recited in Claim 64, wherein said COA information  
8 data includes at least one type of data associated with said COA selected from a  
9 group of COA information data comprising raw optically-detected COA data,  
10 COA related plaintext data, and COA related signature data.

11  
12           66.    The method as recited in Claim 61, wherein said optical data storage  
13 medium includes at least one top surface material, the method further comprising  
14 causing at least one of the following acts to occur:

15               forming said at least one optically-detectable authentication feature  
16 on said top surface material;

17               forming at least one optically-detectable authentication feature  
18 below said top surface material; and

19               forming said at least one optically-detectable authentication feature  
20 such that said optically-detectable authentication feature extends at least  
21 partially into said top surface material.

1           67.    A computer-readable medium comprising computer-implementable  
2 instructions for causing at least one processor to perform acts comprising:

3           writing instructional data for an optical media content protection scheme to  
4 an optical data storage medium, said instructional data being configured to cause  
5 logic associated with an optical media receiving device to operate in accordance  
6 with said optical media content protection scheme when programmed using said  
7 instructional data and accessing associated content data stored on said optical data  
8 storage medium.

9  
10           68.   The computer-readable medium as recited in Claim 67, wherein said  
11 optical media content protection scheme includes a digital rights management  
12 (DRM) protection scheme.

13  
14           69.   The computer-readable medium as recited in Claim 68, wherein said  
15 DRM protection scheme includes at least one marking scheme selected from a  
16 group of marking schemes comprising a data-implemented water marking scheme  
17 and a data-implemented forensic marking scheme.

18  
19           70.   The computer-readable medium as recited in Claim 67, further  
20 comprising:

21           writing at least one type of additional data to said optical data storage  
22 medium, said type of additional data being selected from a group of additional  
23 data comprising substantially unique identifier data associated with said optical  
24 data storage medium, licensing data associated with said optical data storage  
25 medium, and said content data.



1  
2       71.    The computer-readable medium as recited in Claim 67, wherein said  
3 optical data storage medium further includes at least one optically-detectable  
4 authentication feature.

5  
6       72.    The computer-readable medium as recited in Claim 71, wherein said  
7 plurality of optically-detectable authentication features form an optically-  
8 detectable certificate of authentication (COA) and further comprising:  
9       writing COA information data to said optical data storage medium.

10  
11       73.    The computer-readable medium as recited in Claim 72, wherein said  
12 COA information data includes at least one type of data associated with said COA  
13 selected from a group of COA information data comprising raw optically-detected  
14 COA data, COA related plaintext data, and COA related signature data.

15  
16       74.    The computer-readable medium as recited in Claim 71, further  
17 comprising:  
18       generating said COA information data.

19  
20       75.    An apparatus comprising:  
21       non-volatile memory;  
22       an interface mechanism suitable for receiving a removable optical data  
23 storage medium, accessing instructional data associated with an optical media  
24 content protection scheme from said optical data storage medium, and outputting  
25 said accessed instructional data;

1 logic operatively coupled to said interface mechanism and said non-volatile  
2 memory and configured to receive said accessed instructional data and in response  
3 thereto update a current optical media content protection scheme stored in said  
4 non-volatile memory and thereafter while accessing associated content data stored  
5 on said optical data storage medium operatively adhere to said updated current  
6 optical media content protection scheme.

7  
8 76. The apparatus as recited in Claim 75, wherein said current optical  
9 media content protection scheme causes said logic to adhere to a digital rights  
10 management (DRM) protection scheme.

11  
12 77. The apparatus as recited in Claim 76, wherein said DRM protection  
13 scheme includes at least one marking scheme selected from a group of marking  
14 schemes comprising a data-implemented water marking scheme and a data-  
15 implemented forensic marking scheme.

16  
17 78. The apparatus as recited in Claim 75, wherein said interface  
18 mechanism is further configured to access and output to said logic at least one type  
19 of additional data stored on said optical data storage medium, said type of  
20 additional data being selected from a group of additional data comprising  
21 substantially unique identifier data associated with said optical data storage  
22 medium, licensing data associated with said optical data storage medium, and said  
23 content data.

1           79. The apparatus as recited in Claim 75, wherein said interface  
2 mechanism is further configured to detect at least one optically-detectable  
3 authentication feature that is part of said optical data storage medium and output  
4 corresponding information to said logic.

5  
6           80. The apparatus as recited in Claim 79, wherein said optically-  
7 detectable authentication feature includes a plurality of optically-detectable  
8 authentication features forming a substantially unique pattern using at least one  
9 optically detectable material.

10  
11           81. The apparatus as recited in Claim 80, wherein said plurality of  
12 optically-detectable authentication features form an optically-detectable certificate  
13 of authentication (COA).

14  
15           82. The apparatus as recited in Claim 81, wherein said interface  
16 mechanism is further configured to access COA information data stored within  
17 said optical data storage medium and provide said COA information data to said  
18 logic.

19  
20           83. The apparatus as recited in Claim 82, wherein said COA information  
21 data includes at least one type of data associated with said COA selected from a  
22 group of COA information data comprising raw optically-detected COA data,  
23 COA related plaintext data, and COA related signature data.

1           84.    The apparatus as recited in Claim 82, wherein said logic is further  
2 configured to verify said COA information data, and is configured to update said  
3 current optical media content protection scheme stored in said non-volatile  
4 memory once said COA information data has been verified.

5  
6           85.    The apparatus as recited in Claim 84, wherein said interface  
7 mechanism is further configured to access license information data stored within  
8 said optical data storage medium and provide said license information data to said  
9 logic, and wherein said logic is configured to verify said license information data  
10 to determine if content data stored on said optical data storage medium can be  
11 accessed.

12  
13           86.    The apparatus as recited in Claim 85, wherein said logic maintains  
14 license usage information within said non-volatile memory.

15  
16           87.    An apparatus comprising:  
17           an interface mechanism suitable for receiving a removable optical data  
18 storage medium, accessing and outputting data stored thereon, and detecting at  
19 least one optically-detectable authentication feature that is part of said optical data  
20 storage medium and outputting corresponding authentication feature information;  
21           logic operatively coupled to said interface mechanism and configured to  
22 receive said accessed data and said authentication feature information and in  
23 response thereto determine if content data stored on said optical data storage  
24 medium can be accessed.

1        88. The apparatus as recited in Claim 87, wherein said optically-  
2 detectable authentication feature includes a plurality of optically-detectable  
3 authentication features forming a substantially unique pattern using at least one  
4 optically detectable material.

5  
6        89. The apparatus as recited in Claim 88, wherein said plurality of  
7 optically-detectable authentication features form an optically-detectable certificate  
8 of authentication (COA).

9  
10       90. The apparatus as recited in Claim 89, wherein accessed data includes  
11 COA information data having at least one type of data associated with said COA  
12 selected from a group of COA information data comprising raw optically-detected  
13 COA data, COA related plaintext data, and COA related signature data.

14  
15       91. A method comprising:  
16       reading instructional data associated with an optical media content  
17 protection scheme from an optical data storage medium;

18       updating a current optical media content protection scheme based on said  
19 instructional data; and

20       based on said updated current optical media content protection scheme,  
21 determining if a valid license exists prior to accessing associated content data  
22 stored on said optical data storage medium.

1           92.    The method as recited in Claim 91, wherein said current optical  
2 media content protection scheme implements a digital rights management (DRM)  
3 protection scheme.

4  
5           93.    The method as recited in Claim 92, wherein said DRM protection  
6 scheme includes at least one marking scheme selected from a group of marking  
7 schemes comprising a data-implemented water marking scheme and a data-  
8 implemented forensic marking scheme.

9  
10          94.    The method as recited in Claim 93, further comprising accessing at  
11 least one type of additional data stored on said optical data storage medium, said  
12 type of additional data being selected from a group of additional data comprising  
13 substantially unique identifier data associated with said optical data storage  
14 medium, licensing data associated with said optical data storage medium, and said  
15 content data.

16  
17          95.    The method as recited in Claim 91, further comprising detecting at  
18 least one optically-detectable authentication feature that is part of said optical data  
19 storage medium.

20  
21          96.    The method as recited in Claim 95, wherein said optically-detectable  
22 authentication feature includes a plurality of optically-detectable authentication  
23 features forming a substantially unique pattern using at least one optically  
24 detectable material.

1           97. The method as recited in Claim 96, wherein said plurality of  
2 optically-detectable authentication features form an optically-detectable certificate  
3 of authentication (COA).

4  
5           98. The method as recited in Claim 97, further comprising reading COA  
6 information data from said optical data storage medium, said COA information  
7 data including at least one type of data associated with said COA selected from a  
8 group of COA information data comprising raw optically-detected COA data,  
9 COA related plaintext data, and COA related signature data.

10  
11           99. The method as recited in Claim 98, further comprising verifying said  
12 COA information data, and updating said current optical media content protection  
13 scheme once said COA information data has been verified.

14  
15           100. The method as recited in Claim 99, further comprising maintaining  
16 license usage information.

17  
18           101. A method comprising:  
19 receiving a removable optical data storage medium;  
20 detecting at least one optically-detectable authentication feature that is part  
21 of said optical data storage medium;  
22 outputting authentication feature information;  
23 determining if content data stored on said optical data storage medium can  
24 be accessed based at least in part on said authentication feature information.  
25

1           102. The method as recited in Claim 101, wherein said optically-  
2 detectable authentication feature includes a plurality of optically-detectable  
3 authentication features forming a substantially unique pattern using at least one  
4 optically detectable material.

5  
6           103. The method as recited in Claim 102, wherein said plurality of  
7 optically-detectable authentication features form an optically-detectable certificate  
8 of authentication (COA).

9  
10          104. The method as recited in Claim 101, further comprising:  
11          reading COA information data from said optical data storage medium, said  
12 COA information data being associated with said COA and selected from a group  
13 of COA information data comprising raw optically-detected COA data, COA  
14 related plaintext data, and COA related signature data.